

301777



## OFFICE OF BOB BARR

MEMBER OF CONGRESS, 1995-2003

## MEMO

TO : PRIVACY OFFICE, U.S. DEPARTMENT OF HOMELAND  
SECURITY, WASHINGTON, D.C. 20528  
PRIVACY OFFICE, U.S. TRANSPORTATION SECURITY  
ADMINISTRATION, ARLINGTON, VA 22202

FROM : BOB BARR, 21<sup>ST</sup> CENTURY LIBERTIES CHAIR FOR  
FREEDOM AND PRIVACY, THE AMERICAN  
CONSERVATIVE UNION, ALEXANDRIA, VIRGINIA

SUBJECT : COMMENTS REGARDING PROPOSED *SECURE FLIGHT*  
TEST PHASE (DOCKET NO. TSA-2004-19160)

DATE : OCTOBER 22, 2004

TSA - 2004 - 19160 - 452

*Secure Flight Compared to CAPPS II*

While the parameters of the proposed *Secure Flight* program, as reflected in the *Test Phase Privacy Impact Assessment* appear to have addressed some of the privacy, practical and constitutional concerns I and many other individual citizens and organizations noted regarding its now-discredited predecessor, *CAPPS II*, serious problems remain regarding the test phase for *Secure Flight*.

The proposed focus of the *Secure Flight* program appears far narrower than that for *CAPPS II*. This is good. The proposal indicates that passenger names will be compared only to data maintained by the Terrorist Screening Database (TSDB) that consists of persons "known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism." This is far narrower a comparison base than that which was proposed for *CAPPS II*, and therefore would be far less constitutionally- and privacy-suspect than was that discredited program.

MEMORANDUM  
OCTOBER 22, 2004  
PAGE 2

The proposed goal of *Secure Flight* also appears more focused and far less intrusive than that proposed for its predecessor, *CAPPS II*. As set forth in the proposed test phase, *Secure Flight* would not be employed to color code all commercial airline passengers. As proposed, it would in essence be used solely to ensure that no passenger boarding a commercial air carrier in the U.S. is an individual who is a known or suspected terrorist, or a known associate of such a person.

The *CAPPS II* program would have subjected a law-abiding citizen seeking simply to exercise his or her right to travel, to having their name, date of birth, address, Social Security number, and much other personal information run through a secret, "black box" data mining system to then be color-coded according to a secret algorithm. The color code they were then awarded by this black box would determine if they would be allowed to (1) fly subject only to "normal" security measures (green), (2) fly subject to more extensive security measures (yellow), or (3) detained (red). It is hard to imagine a code system, short of tattooing numbers or bar codes on a person's forearm, more un-American than the *CAPPS II* system.

#### Limits Must be Enacted by Statute not Regulation

Lest we become too laudatory of the proposed *Secure Flight* system, however, it must be pointed out that serious questions remain. The only way to ensure this proposed system meets its self-avowed promises to be consistent with constitutional and privacy principles, is to ensure that restrictions on its use and parameters be enshrined not in regulations or policy directives, but in statute.

In the "System Overview" discussion in the test phase proposal, there is a discussion that the only information the TSA will be gathering from the airlines -- and which the airlines would be required to turn over to the government -- will be "full name, contact phone number, mailing address, and travel itinerary." If the government is serious about thusly -- and appropriately -- limiting itself to having access only to information necessary to determine who is flying commercially so it can run their names through the TSDB, then it should not oppose limiting this information by statute; and it ought to be so set forth in statute.

MEMORANDUM  
OCTOBER 22, 2004  
PAGE 3

### "Commercial Data" as a "Back Door"

It also must be pointed out that there is a "back door" contained in the test phase that could render the appropriately limited scope, focus and uses of *Secure Flight* as infirm as its predecessor. Allowing the use of "commercial data" is expressly envisaged in the test phase language. Unfortunately, this would open the door to abuse, and would render essentially meaningless, the privacy and constitutional safeguards proposed in the actual parameters for the program. Any use of commercial data or commercial databases in the test phase or any final implementation of *Secure Flight* should be prohibited by statute.

### Inadequate Process to Correct Errors

The test phase proposal fails to adequately set forth a mechanism whereby disputes might be resolved or through which aggrieved persons could uncover and ensure correction of false, erroneous or mistaken information. Merely reciting that "TSA will create a robust redress mechanism to resolve disputes concerning the Secure Flight program," leaves one with little, if any, sense of security or confidence. This is especially the case considering the government's actual track record in misleading the American public regarding earlier permutations of this and other airline security programs.

Currently, the only effective manner through which a person whose name erroneously shows up on some "no fly list" or "terrorist watch list" can then fly, is if they happen to be of sufficient power that they can call Homeland Security Secretary Tom Ridge; in other words, a person such as Sen. Edward Kennedy or Rep. John Lewis, both of whom have been subject to ridiculous and humiliating airport stops. For the rest of us, once a name gets on a list in error, it's there forever. This is unacceptable, and the *Secure Flight* program should not be allowed to get by with elementary and superficial recitations that there will be a "robust" way to redress errors.

Indeed, even as regards an aggrieved person who might be improperly or erroneously identified as a security threat during this test phase, there is no meaningful mechanism to address, much less correct, problems. Allowing such a person to have access to information in the system "to the greatest extent

MEMORANDUM  
OCTOBER 22, 2004  
PAGE 4

possible and consistent with national security and homeland security requirements" means nothing whatsoever. This language will be employed by the government to deny access on essentially whatever grounds it wants.

#### Limitations on Retention of Data

The time period within which the government will be permitted to retain passenger information must be limited to the duration of the passenger's flight itinerary, by statute. In other words, just as with the Instant Background Check System for firearms purchases, once the government has determined that, for a particular flight, a person does or does not pose a threat - in other words, once it determines if their name is on the TSDB - that should be the end of the matter; the records should not be allowed to be retained beyond that point.

#### Limitations on Data Inputted

Presumably, and appropriately, the information *in* the TSDB will be maintained and continuously updated based on incoming intelligence information; but the fact that "John Doe" elected to travel by air within the United States on such and such an itinerary, should *not* be maintained. Even in this regard, however, in order to ensure constitutional and privacy requirements are met, the information contained in the TSDB must be limited and regulated by law (consistent with national security requirements, of course, which can be done through appropriate statutory language and congressional oversight).